Visual Cryptography and Mixing Techniques for Biometric Privacy

Arun Ross
Associate Professor
Michigan State University
rossarun@cse.msu.edu

http://www.cse.msu.edu/~rossarun
Biometric Data Storage

- Biometric data of an individual is sometimes stored in a central database
- Raises issues related to security and privacy of biometric data
  - Unlike compromised passwords, it is difficult to re-issue biometric data
  - Cross-database matching may be done to track individuals
  - Biometric data mining may be performed to glean information about identity
Preserving Privacy: Face

- **Face De-identification**: Perturb the image so that automated face recognition cannot be reliably done, but preserve details of the face such as expression and gender [Newton et al. (2005), Gross et al. (2006)]

- **Face Swapping**: Protect identity by automatically replacing faces in an image with substitutes taken from a large library of face images [Bitouk et al. (2008)]

- However, in the case of face swapping and de-identification the original face image can be lost
The input image is decomposed and stored in two separate servers: either server will be unable to deduce original identity.
Given an original binary image $T$, it is encrypted in $n$ images, such that:

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \ldots \oplus S_{h_k}$$

where $\oplus$ is a Boolean operation, $S_{h_i}$ is an image which appears as noise, $k \leq n$, and $n$ is the number of noisy images.

This is referred to as $k$-out-of-$n$ VCS.

### 2-out-of-2 VCS

<table>
<thead>
<tr>
<th>Pixel</th>
<th>Probability</th>
<th>Shares #1</th>
<th>Shares #2</th>
<th>Superposition of the two shares</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="white.png" alt="White Pixel" /></td>
<td>$p=0$</td>
<td><img src="black.png" alt="Black Pixel" /></td>
<td><img src="black.png" alt="Black Pixel" /></td>
<td><img src="white.png" alt="White Pixel" /></td>
</tr>
<tr>
<td><img src="white.png" alt="White Pixel" /></td>
<td>$p=\frac{1}{2}$</td>
<td><img src="white.png" alt="White Pixel" /></td>
<td><img src="black.png" alt="Black Pixel" /></td>
<td><img src="black.png" alt="Black Pixel" /></td>
</tr>
<tr>
<td><img src="black.png" alt="Black Pixel" /></td>
<td>$p=0$</td>
<td><img src="black.png" alt="Black Pixel" /></td>
<td><img src="white.png" alt="White Pixel" /></td>
<td><img src="white.png" alt="White Pixel" /></td>
</tr>
<tr>
<td><img src="black.png" alt="Black Pixel" /></td>
<td>$p=\frac{1}{2}$</td>
<td><img src="white.png" alt="White Pixel" /></td>
<td><img src="white.png" alt="White Pixel" /></td>
<td><img src="white.png" alt="White Pixel" /></td>
</tr>
</tbody>
</table>
Sharing a secret image: Binary

- Decomposing a fingerprint into two random images
Gray-level Extended Visual Cryptography Scheme (GEVCS)

- VCS allows us to encode a secret image into \( n \) sheet images
- These sheets appear as a random set of pixels
- The sheets could be reformulated as natural images – known as host images

Visual Cryptography: An Example

PRIVATE IMAGE

HOSTS (PUBLIC IMAGES)

PRIVATE IMAGE

HOSTS AFTER ENCRYPTION

PRIVATE IMAGE AFTER DECRYPTION

HOSTS AFTER ENCRYPTION
Visual Cryptography

Actual Face

AGENCY 1

AGENCY 2
The original image is encrypted into two fixed host images.

<table>
<thead>
<tr>
<th>Original</th>
<th>Hosts</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
<td><img src="image9.png" alt="Image" /></td>
</tr>
</tbody>
</table>
Automated Host Image Selection

- The original image is encrypted into two dynamically selected host images.
Method to protect privacy of face images by decomposing it into two independent host (public) face images

Original face image can be reconstructed only when both host images are available

Either public image does not expose the identity of the original face image
Mixing Fingerprints

- An input fingerprint image is mixed with another fingerprint (e.g., from a different finger)
  - produces a new mixed fingerprint image that obscures the identity of the original fingerprint
- We consider the problem of mixing two fingerprint images in order to generate a new cancelable fingerprint image
Mixing Fingerprints

- Mixing fingerprints creates a new entity that looks like a plausible fingerprint:
  - It can be processed by conventional fingerprint algorithms
  - An intruder may not be able to determine if a given fingerprint is mixed or not
The ridge flow of a fingerprint can be represented as a 2D Amplitude and Frequency Modulated (AM-FM) signal:

$$I(x, y) = a(x, y) + b(x, y)\cos[\Psi(x, y)] + n(x, y)$$

Based on the Helmholtz Decomposition theorem, the phase $\Psi(x, y)$ can be uniquely decomposed into two components:

$$\Psi(x, y) = \Psi_c(x, y) + \Psi_s(x, y)$$

- The continuous component, $\Psi_c(x, y)$, defines the local ridge orientation.
- The spiral component, $\Psi_s(x, y)$, characterizes the minutiae locations.
Fingerprint Decomposition

Original  Spiral Phase  Continuous Phase
Let $F_1$ and $F_2$ be two different fingerprint images from different fingers, and let $\Psi_{c_i}(x, y)$ and $\Psi_{s_i}(x, y)$ be the pre-aligned continuous and spiral phases, $i = 1,2$.

\[
MF_1 = \cos[\Psi_{c_2}(x, y) + \Psi_{s_1}(x, y)]
\]

\[
MF_2 = \cos[\Psi_{c_1}(x, y) + \Psi_{c_2}(x, y)]
\]

The continuous phase of $F_2$ is combined with the spiral phase of $F_1$ which generates a new fused fingerprint image $MF_1$. 
## Mixed Fingerprint Images

<table>
<thead>
<tr>
<th></th>
<th>$F_1$ (FVC2000 DB2)</th>
<th>$F_2$ (WVU)</th>
<th>$MF_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1" alt="F1 Image" /></td>
<td><img src="image2" alt="F2 Image" /></td>
<td><img src="image3" alt="MF1 Image" /></td>
</tr>
<tr>
<td></td>
<td><img src="image4" alt="F1 Image" /></td>
<td><img src="image5" alt="F2 Image" /></td>
<td><img src="image6" alt="MF1 Image" /></td>
</tr>
<tr>
<td></td>
<td><img src="image7" alt="F1 Image" /></td>
<td><img src="image8" alt="F2 Image" /></td>
<td><img src="image9" alt="MF1 Image" /></td>
</tr>
<tr>
<td></td>
<td><img src="image10" alt="F1 Image" /></td>
<td><img src="image11" alt="F2 Image" /></td>
<td><img src="image12" alt="MF1 Image" /></td>
</tr>
</tbody>
</table>
# Mixed Fingerprints

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_1$</td>
<td>$F_2$</td>
<td>$MF_1$</td>
<td>$MF_2$</td>
</tr>
<tr>
<td><img src="image1.png" alt="Image 1" /></td>
<td><img src="image2.png" alt="Image 2" /></td>
<td><img src="image3.png" alt="Image 3" /></td>
<td><img src="image4.png" alt="Image 4" /></td>
</tr>
<tr>
<td>$F_1$ (FVC2000 DB2)</td>
<td>$F_2$ (WVU)</td>
<td>$MF_{12}$</td>
<td><img src="image5.png" alt="Image 5" /></td>
</tr>
</tbody>
</table>

- **WVU with WVU**
- **WVU with FVC**

© Ross 2013
Mixing Fingerprints: Results

- Can the mixed fingerprint be used as a new biometric indicator? (Yes)
- Are the original fingerprint and the mixed fingerprint correlated? (No)
- Does mixing result in cancelable templates? (Yes)
- If two different fingerprints are mixed with a common fingerprint, are the mixed fingerprints similar? (No)
Visual Cryptography for decomposing a face and storing it in two separate servers

- Individual servers cannot identify the face

Mixing fingerprints by combining the spiral and continuous phase components of two fingerprint images

- Cancellable fingerprints

- Joint identity/Group Authentication
[Projects Funded by NSF CAREER Award]